

METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR
MULTI-PACKET MESSAGE AUTHENTICATION FOR SECURED SSL-
BASED COMMUNICATION SESSIONS

Abstract of the Disclosure

Methods, systems and computer program products are provided of message authentication for an SSL-based protocol connection between a source device and a destination device. A group message authentication code (MAC) is generated
5 based on a plurality of communication packets. Each of the communication packets has at least one data record. The plurality of communication packets is transmitted using the SSL-based protocol connection along with the generated group MAC. Individual ones of the plurality of communication packets do not include an associated packet MAC as transmitted. A data record count to a next
10 group MAC may be transmitted before transmitting the data records corresponding to the data record count and transmitting the next group MAC. The data records of the communication packets may be pre-encrypted and transmitted using the SSL-based protocol connection to encrypt the group MAC but not the data records. Receiver side methods, systems and computer program products are also provided.